# UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Premises located at 1322 South Cesar E. Chavez Drive, Milwaukee, WI 53204, more particularly described in Attachment A.

Case No. 17-M-219

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ■ contraband, fruits of crime, or other items illegally possessed;
- ■ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 641 (Theft of government property); and 26 U.S.C. § 7062(2) (Aid and assist in the preparation of false income tax returns)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Special Agent Park Jones, IRS
*Printed Name and Title*

Sworn to before me and signed in my presence:

Date: Dec. 19, 2017

*Judge's signature*

City and State: Milwaukee, Wisconsin

Honorable David E. Jones, U.S. Magistrate Judge
*Printed Name and Title*

## AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

I, Park Jones, having been duly sworn on oath, state as follows:

### Affiant's Background

1. Your affiant is employed as a Special Agent with the Internal Revenue Service, Criminal Investigation (IRS-CI) and has been so employed since September 2005. As a Special Agent, my responsibilities include the investigation of potential criminal violations of the Internal Revenue Code under Title 26 of the United States Code as well as related Title 18 and Title 31 offenses.

2. The facts in this affidavit are from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Your affiant is knowledgeable of the characteristics of an Individual Taxpayer Identification Number ("ITIN") tax refund scheme and has been involved in investigating a multi-million dollar ITIN tax refund scheme in Milwaukee, Wisconsin. Since 2013, your affiant and other investigating agents have conducted 22 search and seizure warrants which has resulted in the seizure of approximately $1.8 million in cash, $1.0 million in U.S. Treasury checks, and voluminous financial/tax documents indicating evidence of fraudulent tax return activity involving ITINs.

4. Based upon my training and experience, individuals who amass proceeds from illegal activities routinely attempt to further that conduct and/or conceal the existence and source of their funds through financial transactions.

5. Individuals involved in both legal and illegal activities maintain books and records of some kind (i.e. either formal or informal). These records include notebooks, payment ledgers, bank statements, and records showing the receipt and disposition of funds. Records of this type are normally kept for extended periods of time, are portable and routinely stored in places that are secure, but easily accessible, such as their personal residence, an associate's residence, or personal vehicle. Likewise, it is common for businesses who engage in transactions with individuals involved in criminal activity to conceal the nature of transactions through false transactional records, by maintaining false financial records, or placing the transaction in a nominee name. These businesses may need to keep these false records for bookkeeping reasons. However, these false records may be placed in a separate location such as a personal residence, safe or safe deposit box for concealment.

**Purpose of Affidavit**

6. Based on the totality of the facts and circumstances contained in this affidavit, I submit there exists probable cause to believe that Marianyela Salas Aguilar (Salas) and Sonia Aguilar (Aguilar) and others have been involved in a scheme to defraud the United States by conspiring to embezzle, steal, purloin, and knowingly convert the proceeds of tax refund checks to their own use, in violation of 18 U.S.C. §§ 371 and 641, and Title 26 U.S.C. § 7206(2), aid and assisting in the preparation of false tax returns.

7. Based on the information contained herein, I submit there is probable cause to believe evidence and/or the instrumentalities of criminal activities will be found at the following locations:

- 1322 South Cesar Chavez Drive, Milwaukee, Wisconsin.
- 1133 W. Lincoln Avenue, Milwaukee, Wisconsin.

The location will be hereinafter referred to as the PREMISES, and is more fully described in Attachment A.

8. More specifically, there is probable cause to believe that the items listed in Attachment B to the search warrant will be found at these locations.

9. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the issuance of a search warrant, I have not included each and every fact I know about this investigation. Rather, I have set forth only the facts that I believe are necessary to establish a finding of probable cause to support the issuance of a search warrant for the identified locations.

**IRS Regulations and Provisions**

10. Every person who earns United States (U.S.) source income is required to pay taxes. U.S. citizens are required to pay taxes on worldwide income from whatever source derived. The IRS typically treats any individual living in the U.S., either legally or illegally, as a resident alien who is taxed on worldwide income and required to file an income tax return just like any US citizen.

11. Every person who files a U.S. income tax return must provide a taxpayer identification number when the person files a return. For American citizens or resident aliens who entered the United States legally, this would typically be a Social Security Number (SSN). However, individuals, such as resident and non-resident aliens who are not eligible for a SSN, must apply for an ITIN. An ITIN is for tax use only and does not change a taxpayer's immigration status or his/her legal right to work in the U.S. An ITIN can be distinguished from an SSN because the first number is a nine and the middle two-digit number is between 70-99, excluding numbers 89 and 93. Only resident aliens and nonresident aliens (having earned

income in the United States and therefore required to file a federal individual income tax return) who do not have, and are not eligible for, a social security number may apply for an ITIN.

12. In order to obtain an ITIN, a taxpayer must submit to the IRS an Application for IRS Individual Taxpayer Identification Number, Form W-7, and an original valid U.S. Federal Income Tax Return or documentation explaining the exception to the tax return requirement. In addition, the following documents of personal identifying information (PII) must be submitted:

- An original passport or;
- A combination of two or more Personally Identifying Information ("PII") documents that show the taxpayer's name and photograph (with the exception of children under the age of 14). These documents include: United States Citizenship and Immigration Services photo ID; national ID card; Visa issued by the US; US or Foreign Driver's License; US or Foreign Military Card; foreign voter ID card; birth certificate; school records (if under the age of 14); medical records (if under the age of 6); and/or some other identifying document. In lieu of originals, the taxpayer may provide copies that are certified by the issuing agency.

13. The Preparer Tax Identification Number (PTIN) is an identification number that all paid tax return preparers must use on U.S. federal tax returns or claims for refund submitted to the IRS. Anyone who, for compensation, prepares all or substantially all of any federal tax return or claim for refund must obtain a PTIN issued by the IRS.

14. Federal legislation mandates anyone filing more than 10 federal tax returns to electronically file the returns with the IRS. IRS accepts electronic submission of a variety of tax forms through their IRS Authorized e-file Providers. An Electronic Filing Identification Number (EFIN) is a number issued by the IRS to individuals or firms that have been approved as Authorized IRS e-File providers.

15. IRS Circular 230, which prescribes the rules and responsibilities for those who practice before the IRS, states that under §10.31, a practitioner may not endorse or otherwise negotiate any check (including directing or accepting payment by any means, electronic or

otherwise, into an account owned or controlled by the practitioner or any firm or other entity with whom the practitioner is associated) issued to a client by the government in respect of a Federal tax liability.

**Facts Supporting Finding of Probable Cause**

16. The IRS has identified ITIN tax refund schemes involving false Forms W-7 and false individual income tax returns perpetrated throughout the country. The characteristics of an ITIN tax refund scheme include:

- Filing of U.S. Individual Income Tax Returns (Forms 1040, 1040A and/or 1040EZ);
- Use of Hispanic surnames for taxpayer names;
- Filing Status as Head of Household;
- False wage and income tax withholding amounts on the tax returns that cannot be verified through contacts with the named employer or by searches in the IRS's database for matching wage information filed by the named employer;
- Use of numerous dependents to claim multiple dependency exemptions and increase the Additional Child Tax Credit (ACTC). The ACTC is a refundable tax credit which was intended by the U.S. Congress to lower the tax burden of families who are raising children. As a credit, the ACTC reduces tax liability dollar for dollar. As a refundable credit, the unused portion of the ACTC may be refunded to a qualifying taxpayer. Thus, even if an individual is not required to file a federal income tax return, an individual who qualifies for the ACTC can file a tax return claiming the ACTC and receive a refund for the ACTC;
- Tax refund claims that request paper federal tax refund checks to be mailed to the purported taxpayer addresses, as opposed to requesting direct deposits into a traceable bank account. Perpetrators are known to search the IRS website to learn when the IRS has issued the fraudulently obtained tax refund checks so that the perpetrator knows when to obtain the check at the address used.

17. Based on my personal knowledge and information shared with me by other law enforcement officers, I know the following regarding ITIN tax refund schemes:

- An ITIN scheme involves four basic participants: 1) the source, 2) the return preparer, 3) the runners, and 4) the ringleader. The source is the person who

procured the PII and transferred it to the return preparer. The return preparer is the person who actually files the fraudulent tax returns. The runners gather the proceeds (i.e. cash fraudulent refund checks). In larger schemes, the ringleader is the person organizing the entire operation and the ringleader's name may not appear on any document. In smaller schemes, the same person may fulfill multiple roles.

- Individuals residing in Mexico are paid a minimal amount of money ($100-$150) for turning over their PII documents to scheme participants. The documents are then shipped to the United States for the purpose of securing an ITIN number and filing a fraudulent tax return;

- Tax returns are filed with false wages derived from fraudulent Forms W-2 wage documents;

- Typically, the tax refund claims are filed by mail, with no return address, making the returns difficult for authorities to trace;

- Repeated use of identical addresses for multiple distinct taxpayers, at which there is no history of the taxpayer actually residing;

- Fraudulently obtained tax refund checks are cashed with the assistance of conspiring employees at banks or Money Service Businesses (MSBs), who generally do not require the payee named on the face of the check to appear at the time the check is cashed. In some instances, false identification documents may be presented.

18. According to online corporate records in the State of Wisconsin, Nuestros Envios LLC was registered in December 2014. The registered agent for the business was Salas with an office address of 1322 South Cesar Chavez Drive, Milwaukee, Wisconsin. In addition, a source of information told your affiant that Nuestros Envios is owned by Aguilar and her daughter, Salas.

19. Money Mart LLC was registered in the State of Wisconsin as an entity in December 2015. Money Mart LLC registered with the Financial Crimes Enforcement Network as a money service business in February 2016. The president and owner is listed as Rodolfo Salas Camacho. Camacho lists the business address as 1322 South Cesar Chavez Drive, Milwaukee, Wisconsin.

20. IRS records show Salas was issued a PTIN on January 22, 2016 and an EFIN on February 19, 2016.

21. The IRS conducts Bank Secrecy Act ("BSA") compliance exams of Money Service Businesses to assess compliance with the regulatory requirements pertaining to the Bank Secrecy Act. The IRS conducted a compliance exam of Money Mart for the period of February 1, 2016 to July 31, 2016. The exam was closed out in August 2017. According to the BSA auditor conducting the compliance exam, the owner of Money Mart LLC is Rodolfo Salas Camacho, the step father of Salas and ex-husband of Aguilar. Salas is the manager of Money Mart. Money Mart was previously known as Nuestros Envios LLC. Nuestros Envios started in 2014 but rebranded itself under the name Money Mart. Money Mart has locations at 1322 South Cesar Chavez Drive and 1133 West Lincoln Avenue in Milwaukee, Wisconsin.

22. The BSA auditor described the procedures Money Mart LLC has in place when customers present a check for cashing. Money Mart LLC uses an electronic check cashing system, Emaginenet, for managing the check cashing process. The customer will present a valid identification document ("ID") such as a driver's license, state ID, or foreign ID. The ID information will be entered and scanned into Emaginenet. A copy of the cashed check is scanned into the system along with a digital picture of the customer conducting the transaction. The system can then build a customer history for each time a transaction is conducted by the customer.

23. The BSA auditor performed a cash flow analysis of Money Mart LLC for the period February 2016 to July 2016. The analysis compared the dollar amount of cashed checks in the Emaginenet system to the amount of cash withdrawals at the Money Mart business bank account. A summary of the analysis is below:

| | | |
|---|---|---|
| Sources of Cash According to Business Bank Account: | | |
| Money Order Sales | | $ 148,395.23 |
| Wire Sends | | 518,018.00 |
| Wire Fees | | 12,968.90 |
| Check Cashing Fees | | 29,833.16 |
| Cash from Bank | | 3,669,000.00 |
| Total Sources of Cash | $ | 4,378,215.29 |
| Uses of Cash According to Emaginenet System: | | |
| Check Cashed | | $ 2,983,315.60 |
| Total Uses of Cash | | $ 2,983,315.60 |
| Overage | $ | 1,394,899.69 |

24. The above suggests Money Mart LLC cashed $1.3 million of checks that were not accounted for in the Emaginenet check cashing system.

25. Your affiant also conducted a sampling of one hundred twenty-nine (129) federal tax refund checks totaling approximately $392,000 which were cashed and cleared through the Money Mart LLC business bank account from February 2016 to July 2016. Based upon records obtained during the compliance audit, only thirty (30) of those federal tax refund checks totaling approximately $66,000 were recorded in the Emaginenet check cashing system. In other words, Money Mart LLC cashed ninety-nine (99) federal tax refund checks from February 2016 to July 2016 without using its Emaginenet check cashing system.

26. Your affiant and other investigating agents conducted an investigation of ITIN scheme participant Amalia Gamboa. On October 31, 2017, in case number 17-CR-78, Gamboa pleaded guilty to identity theft, mail fraud and theft of government property charges stemming from her involvement in the ITIN fraud scheme, in violations of 18 U.S.C. § 641, 1028A, and 1341. As a result of her scheme, Gamboa received and presented for cashing approximately $5.1 million worth of fraudulently obtained tax refund checks.

27. During the investigation of Gamboa, your affiant and other investigating agents conducted numerous surveillances of Gamboa in the fall of 2015. The surveillances identified several residences in Milwaukee that Gamboa was using as controlled addresses to receive fraudulent tax refund checks. These addresses were as follows:

- 643/645 West Bruce Street.
- 1602 South Muskego Avenue
- 1015 South 15th Street
- 1556 South 14th Street

28. Your affiant conducted an analysis of tax returns filed with the IRS for the period January 2015 to October 2015 associated with the addresses at which Gamboa was observed in the fall of 2015. Based on information obtained from the IRS, your affiant is aware of the following:

- 102 tax returns with tax refunds totaling over $474,000 were filed with the IRS using the 643/645 West Bruce Street, Milwaukee, Wisconsin as the address.
- 81 tax returns with tax refunds totaling over $342,000 were filed with the IRS using the 1602 South Muskego Avenue, Milwaukee, Wisconsin as the address.
- 71 tax returns with tax refunds totaling over $328,000 were filed with the IRS using the 1015 South 15th Street, Milwaukee, Wisconsin as the address.
- 34 tax returns with tax refunds totaling over $163,000 were filed with the IRS using the 1556 South 14th Street, Milwaukee, Wisconsin as the address.

29. Your affiant conducted an analysis of the canceled tax refund checks associated with the tax returns in the paragraph #28. Approximately eighty (80) of the tax refund checks, totaling over $368,000, were cashed at Nuestros Envios LLC in August, September and October 2015.

30. In addition, during a surveillance in October 2015, your affiant and other IRS-CI agents followed Gamboa to a residence in West Allis, Wisconsin. In the driveway of the residence, a vehicle registered to Aguilar was parked in the driveway. The vehicle was

registered to Aguilar but Salas was known to drive the vehicle. Gamboa stayed at the residence for over 2 hours. Neither Gamboa or Aguilar were or had permanently resided at the residence. Based on information gathered in this investigation, investigating agents believe this residence could have been a "meet" location for Aguilar/Salas and Gamboa to exchange money from the fraudulently obtained tax refund checks.

31. In December 2015, IRS-CI agents executed search warrants at Soraida Nunez's business and residence. Nunez is under criminal investigation for violations of 18 U.S.C. §§ 286, 287, 371 and 641, and 26 U.S.C. § 7206(2) related to the ITIN fraud scheme. Shortly after execution of the warrants, it is believed Nunez fled to Mexico. IRS-CI Special Agent Patrick Debbink received a letter postmarked January 12, 2016, from Nunez. In the letter, Nunez describes her involvement in the tax fraud scheme. Also, Nunez provided a list of people committing ITIN tax fraud in Milwaukee.

32. Nunez stated in the letter that Salas has a new business called Nuestros Envios which is used to cash the checks for the individuals on her list. Salas charges 25% to cash the checks and an extra $100 per check if she delivers the cash directly to the scheme participant. Later in the letter, Nunez stated that if investigating agents surveil Salas agents will identify numerous scheme participants because Salas obtains the tax refund checks from scheme participants, cashes the checks, and then meets the scheme participant in restaurants to deliver the cash.

33. IRS-CI has been investigating Alberto Fernandez Ramirez (Ramirez) and his wife, Ana Delia Dominguez (Dominguez) for attaining over $1.6 million in fraudulently obtained tax refund checks from the ITIN tax refund fraud scheme.

34. During the investigation of Ramirez, IRS-CI Special Agent Patrick Debbink observed meetings between Aguilar and Ramirez. On March 7, 2016, Aguilar was followed to 2037/2039 South 13th Street in Milwaukee, Wisconsin (Ramirez's residence). Aguilar was observed entering 2037 South 13th Street without knocking or ringing a door bell. Aguilar stayed at the residence for over two hours. Aguilar's vehicle was observed on four other occasions in March and April 2016 parked in the vicinity of 2037/2039 South 13th Street, Milwaukee, Wisconsin.

35. In May 2017, your affiant conducted three (3) search warrants at locations connected to Ramirez and Dominguez, including the 2037/2039 South 13th Street location where agents had previously observed Aguilar enter.

36. During the search of the Dominguez's business located at 1129 West Lincoln Avenue, agents seized financial records in the name of Money Mart and/or Salas establishing a relationship between Ramirez/Dominguez and Salas/Aguilar. The records are summarized as follows:

- A letter from the IRS addressed to M Tax & Financial Services / Marianyela Salas Aguilar Sole MBR [Member] / 1133 West Lincoln Avenue, Milwaukee, Wisconsin. The letter assigns Employer Identification Number 81-1537226 to Salas.

- A lease agreement entered between Salas and a landlord for 1133 West Lincoln Avenue, Milwaukee, Wisconsin. The lease agreement is signed by Salas.

- Articles of Incorporation for M Tax & Financial Services LLC. The organizer or sole member is listed as:

  Marianyela Salas Aguilar
  1322 South Cesar Chavez Drive
  Milwaukee, Wisconsin 53204

- Eleven (11) BMO Harris debit transaction records for Money Mart LLC, 1322 S Cesar Chavez Drive, Milwaukee, Wisconsin.

- A letter from AT&T addressed to Salas.
- A copy of a federal tax refund check issued on March 17, 2017 and a mailing address of 1133 West Lincoln Avenue, Milwaukee, Wisconsin.

37. During the search of Ramirez's residence, a lease rental agreement record for a storage unit was located in the kitchen of the residence. The agreement was in a nominee name but paid for by Ramirez and Dominguez. The nominee was interviewed and stated Dominguez asked the nominee to open a storage locker in the nominee's name. Dominguez traveled with the nominee to the storage facility to sign the rental agreement. The nominee has never been inside the rented locker or made a payment for the unit. Your affiant obtained a search warrant for the storage locker. Inside the storage locker, SAs seized several folders containing tax returns and ITIN documents.

38. On twelve (12) of the tax returns, the Paid Preparer section was completed. The Paid Preparer section identifies the individual who prepared the tax return. The twelve (12) returns listed Salas as the individual who prepared the returns at Money Mart located at 1133 West Lincoln Avenue, Milwaukee, Wisconsin.

39. In addition, on three (3) of the returns described in the paragraph above, the taxpayer residential address listed on the return was also 1133 West Lincoln, Milwaukee, Wisconsin. Thus, any tax refunds issued with the filed tax return would be sent directly to Money Mart at 1133 West Lincoln Avenue, Milwaukee, Wisconsin.

40. Your affiant conducted a search of IRS records for tax returns using the addresses of Ramirez/Dominquez (1129 West Lincoln Avenue, Milwaukee, Wisconsin and 2037/2039 South 13th Street, Milwaukee, Wisconsin) and filed by Salas. From February 11, 2017 to March 15, 2017, six (6) ITIN tax returns were filed with the IRS with those characteristics. All of the returns claimed a tax refund which totaled approximately $29,000. The IRS issued one refund

for the filed returns. The refund was cashed at Money Mart.

41. Your affiant conducted a search of IRS records for tax returns using the address of 1133 West Lincoln Avenue, Milwaukee, Wisconsin. From February 10, 2017 to April 8, 2017, thirty-one (31) ITIN tax returns were filed with the IRS using that address. All of the returns claimed a tax refund which totaled approximately $128,000. The IRS posted the filed returns but held twenty-eight (28) tax refunds until the taxpayer listed on the return could verify their identity. The IRS never received any correspondence from any of the (28) taxpayers verifying their identity. The IRS did issue refunds on three (3) of the tax returns. All three (3) of the tax refunds were cashed at Money Mart.

42. Your affiant has reviewed a sample of the tax return data associated with the returns filed using the addresses of 1129 West Lincoln Avenue, 2037/2039 South 13th Street and 1133 West Lincoln Avenue. The data has the characteristics of the ITIN fraud scheme described in paragraph #17.

43. Your affiant has reviewed the bank records associated with Nuestros Envios LLC and Money Mart, LLC for the previous tax filing year of 2016. In February and March 2016, 3 tax refund checks were deposited into the Money Mart LLC bank account with an address of 2037 South 13th Street, Milwaukee, WI. One tax refund check was deposited into the same account using an address of 2039 South 13th Street, Milwaukee, Wisconsin. Both of those addresses are the residents of Ramirez and Dominguez.

44. In March and April 2016, 10 tax refunds totaling $62,505 were deposited into the Money Mart LLC bank account with taxpayer addresses of 1129 West Lincoln Avenue, Milwaukee, Wisconsin. That address is the business operated by Dominguez.

**Computers, Electronic Storage, and Forensic Analysis**

45. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES described in Attachment A, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. *Probable Cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

47. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

48. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

49. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

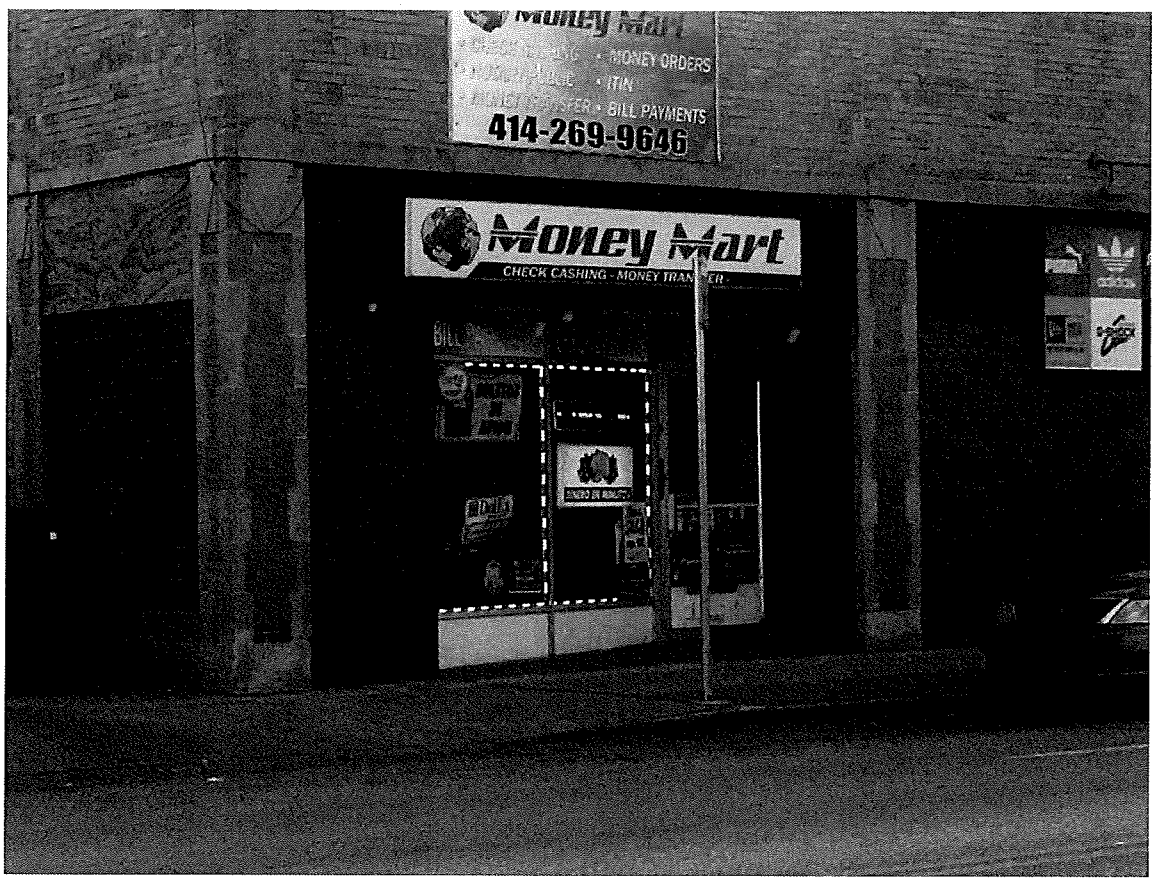
**Conclusion**

50. Based on the facts set forth above, your affiant submits that probable cause exists to believe the individuals described above and others have violated 18 U.S.C. §§ 371 and 641, and Title 26 §7206(2) and that evidence of the aforementioned violations can be found at the PREMISES, more fully described in Attachment A.

51. Your affiant respectfully requests that a search warrant be issued authorizing the search of the premises for items described in Attachment B, which constitute evidence, fruits, and instrumentalities of the criminal offenses described in this Affidavit.

# Attachment A

1322 South Cesar E Chavez Drive, Milwaukee, WI – The building is a business with a brown brick exterior and a large glass window. The building has two signs affixed to the exterior of the building. The first sign has "Money Mart" in blue letters. A second sign is located directly above the first sign and has "Money Mart" in black letters.



**ATTACHMENT B**

ITEMS TO BE SEIZED

Evidence to be seized includes the following records, documents and/or other materials relating to the period December 1, 2014, through the date of the execution of the warrant, in any form (written, printed, magnetic or electronic) including:

1. Original or copies of United States Treasury Checks.

2. Original or copies of Passports; Driver's Licenses; Resident Alien Cards; Immigration Cards; Social Security Cards: Voter Identification Cards; any other documents used to cash United States Treasury Checks.

3. Original or copies of Forms W-7, Application for IRS Individual Taxpayer Identification Number, together with all supporting documentation and attachments thereof.

4. Original or copies of U.S. income tax returns with all forms, worksheets, schedules, and attachments thereof.

5. Original or copies of Forms W-2, Wage and Tax Statements.

6. Internal Revenue Service correspondence.

7. Internal Revenue Service publications, pamphlets, forms, regulations, or extracts from the Internal Revenue Code.

8. Books, records, notes, notebooks, correspondences, travel records, mailings, photographs, letters, facsimiles, documents, and other items used to maintain a record of tax returns filed and tax refund checks cashed.

9. Accounting records, specifically financial statements, ledgers, journals, check registers, and other books and records used to maintain a record of income and expenses.

10. Checking, savings and investment account records, including signature cards, account statements, deposit receipts, withdrawal receipts, cancelled checks, money orders, cashier's checks, records of incoming and outgoing wire transfers, electronic funds transfer records, checkbooks, credit card records and receipts, including supporting documentation and schedules, and any other records of documents pertaining to the receipt, expenditure, or concealment of money.

11. Financial records which may show wealth or acquisition of assets, to include, but not limited to, real estate documents, safety deposit box keys and records, titles to assets, vehicle identification numbers, asset serial numbers, asset model numbers, loan documents, mortgage records, personal financial statements, travel or vacation records,

insurance records, wills, trust documents, and financial instruments such as certificates of deposit, IRA's, bonds, and passbooks.

12. Computers or storage media used as a means to commit or store evidence of the violations described in the affidavit.

13. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the computer user;

    e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

    f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

    h. evidence of the times the COMPUTER was used;

    i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

    j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

14. All cash and currency.